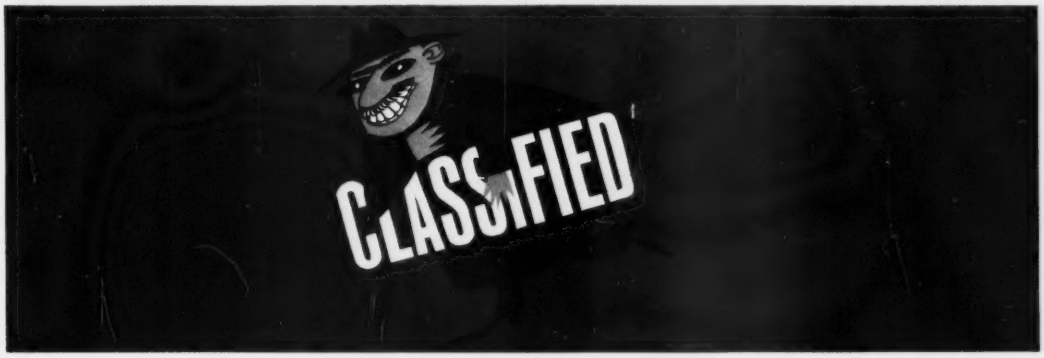
SAFEGUARD ALL CLASSIFIED MATERIAL !



...remember, somebody else wants it !

COMMANDERS DIGEST

DEPARTMENT OF DEFENSE • WASHINGTON, D.C.

Vol. 13, No. 2 **November 16, 1972**

New Security Classification System Announced

Effective June 1, 1972, by E. O. 11652 and a supplementing National Security Council Directive, the President changed and revitalized the security classification system of the Government. The Department of Defense responded by issuing DoD Directive 5200.1 and DoD Information Security Program Regulation 5200.1-R.

It is vitally important that DoD personnel everywhere, military and civilian, be well versed in the new system and put into practice to the best of their ability. Much that is new must be learned. Much that is old must be discarded.

Because commanders everywhere perform a leadership role in implementing DoD programs, I have authorized these two special issues of the COMMANDERS DIGEST to emphasize the importance of the new DoD security classification system. I strongly urge each commander who receives copies of the special issues to master their content—and to motivate his colleagues to do likewise in order that the Program will be administered efficiently and effectively.

A well-managed progressive Program will obviously accomplish the President's objectives. Consistent with the interests of national security, more information will be made available to the general public, DoD technology will be more effectively transferred within Government and the private sector, technology communications barriers with our allies will be further reduced, and international cooperation enhanced.

MELVIN R. LAIRD
Secretary of Defense

During Pentagon Interview

Officials Explain Regulation Changes

David O. Cooke, Deputy Assistant Secretary of Defense for Administration, and Joseph J. Liebling, Deputy Assistant Secretary of Defense for Security Policy, were interviewed concerning the Defense Department's new classified information regulation.

The interview:

* * * * *

Q. Mr. Liebling, can you outline for us the purpose of the new Department of Defense Regulation on classified information?

A. Yes, the initial purpose, of course, is to implement the Executive Order approved by the President on March 8 and the implementing instructions issued by the National Security Council on May 17. Simply stated, it provides for the classification of less information, the declassification of more information, plus a monitoring system for effective compliance. The principal objective of the new regulation is, of course, to make the greatest amount of information available to the public.

Q. The charge then that has been levied in some quarters that it is designed to hide information from the United States public is not valid.

A. (Mr. Liebling) On the contrary, it is designed by its provisions to progressively downgrade and declassify more information so that it is accessible to the public.

POINT OF INTEREST. David O. Cooke (left), Deputy Assistant Secretary of Defense (Administration), emphasizes a point of concern in a discussion with Joseph J. Liebling, Deputy Assistant Secretary of Defense (Security Policy), at a Pentagon meeting. (Official USAF Photo)

Q. Mr. Cooke, in your judgment, why was it necessary to develop a new regulation?

A. The old Executive Order had been in effect in various modifications since the early 1950s, and there had been, I think, experiences with it which suggested that the maximum amount of information was not being made available to the public. There had been charges, some of them well-founded, that various officials were hiding behind the skirts of the Executive Order to withhold information. However, I would like to emphasize that when Secretary Laird took over, he expressly said that the classification system in Defense would not be used to conceal mistakes, even when disclosures would result in embarrassment. I think, in essence, President Nixon decided it was time for a new look, a fresh approach to this problem. Because of his concern, the President ordered a study in January 1971 which led to the new Executive Order.

Q. Mr. Cooke, how long does it take a classified document to be declassified?

A. This depends on the level of classification. As you know, documents can be classified at one of three levels: Top Secret, Secret, or Confidential, in descending order. The new Executive Order sharply decreases the time for automatic declassification, so that a Top Secret document—with few exceptions—would be downgraded to Secret at the end of two years, to Confidential at the end of two additional years, and declassified at the end of six additional years. The Executive Order also provides that, if the originator of a document can predict a date or an event which is shorter than these time periods, the document will be declassified on the occurrence of that date or event.

Q. If I wish to see a particular classified document, what is the procedure that I have to go through, and when could I request it? Using, as an example, something from World War II.

A. (Mr. Cooke) Many World War II documents are now approaching 30 years

COMMANDERS DIGEST

A publication of the Department of Defense to provide official and professional information to commanders and key personnel on matters related to Defense policies, programs and interests, and to create better understanding and teamwork within the Department of Defense.

Published weekly by the American Forces Press Service, 1117 N. 19th St., Arlington, Va. 22209, a unified activity of the Office of Information for the Armed Forces, OASD (M&RA). Reproduction of content is authorized.

Telephones: (202) OXford 4-4912
Autovon 224-4912

old. The new Executive Order provides that a member of the public can request a classification review of any document over ten years old, including World War II documents, providing he can identify the document with a sufficient degree of particularity, and we can locate it without an undue effort. This classification review is conducted with a view toward the declassification of that document and making it available for public release. I think it is important to note that during such reviews the burden of proof is on those who would say, "No, it is still classified." Also, as you are probably aware, there has been a program for some time under the Archivist of the United States to declassify records of the World War II era.

Q. Mr. Cooke, who is authorized under the new Directive to make classification determinations?

A. I take it that you are talking about who can classify a document. First of all, somebody has to make an initial or original determination that the information in a document should be Top Secret, Secret or Confidential, or should not be classified at all. Within the Department of Defense the number of people who can make that decision under the new Executive Order has been sharply reduced. Mr. Liebling, do you recall the exact figures?

Mr. Liebling: Yes, the number of persons authorized to classify in all three categories has been reduced by more than 71 percent. Specifically, in the Top Secret category, we dropped from almost 900 to less than 600. At the same time, there are only about 3,700 authorized to classify in the Secret category and approximately 4,500 in the Confidential category. These figures represent a total reduction of original classifiers from about 30,000 to less than 9,000. As you can see this is quite a significant decrease and obviously has the effect of preventing a greater amount of information from being classified, which is a prime objective of the program.

Q. Is this authority centralized within DoD or is it dispersed widely?

A. (Mr. Liebling) No, the authority is not centralized, it is dispersed on a worldwide basis. However, it is purposely limited to only those people who absolutely require the authority for effective administration. Top Secret classification authorities for instance, must be designated at the Secretariat level. Within the Office of the Secretary of Defense, this authority has been limited to Principal Assistants and Assistant Secretaries of Defense. Incidentally, only 21 at that level have been granted Top Secret classification authority. Only 592 persons on a worldwide basis have been granted this level of classification authority.

Q. Is there a possibility that this narrower scope can result in a delay in the issuance of classified documents?

A. (Mr. Liebling) No, not at all. By

limiting the scope, we have more sharply defined the authority for approval in particular activities. Most people who generate a document with classified information in it are merely classifying that information on a judgment that has been exercised by somebody else. What we are trying to do is to establish a reasonable authority basis with a fixed responsibility, which is one of the most significant aspects of the program, as Mr. Cooke alluded to before. In other words, the burden of proof is on the classifier. And, the intent of the program, of course, is to locate the man who actually affixed the classification based on other sources, or is responsible for the classification in the first place. While it is true fewer persons are now permitted to exercise classification authority, there shouldn't be any appreciable loss of time in getting someone to authenticate a classification.

Mr. Cooke: Classification authority is not always required when you prepare a classified document. For instance, if you were to write a memorandum and you used as your source documents, three Top Secret documents, it would not be necessary for you to identify yourself as the classifier of the memorandum. In this instance, you would not be exercising classification authority, you would simply be borrowing and applying the classification decision of an official who had the authority to do so, and he is the one who would be identified as the classifier.

Q. Mr. Cooke, recently there have been a number of charges from people outside the Defense Department that there is a tendency to overclassify material. Do you agree?

A. Yes, I do to some extent, and this was particularly true under the old Executive Order in the sense that very few, if any, people were reprimanded for overclassifying. I think there is a natural tendency on the part of someone who is preparing a memorandum from classified documents to say, "Well, I'm not sure whether it is Secret or Confidential, but let's be safe, and call it Secret." This possibility, to a degree, has been reduced under the provisions of the new Executive Order and its implementing Directives. Under the monitoring system referred to earlier, the new Executive Order provides for the possibility of administrative penalties for overclassification. This is the first time I am aware of that an Executive Order has talked about administrative penalties for overclassifying and underclassifying in addition to the criminal statutes for unauthorized disclosures which have always applied.

Mr. Liebling: In fact, the policy expressly states that if you are in doubt as to which degree of classification to apply, you will use the least restrictive.

Q. How do the administrative penalties differ from the criminal penalties and how would they be applied?

A. (Mr. Cooke) In the case of uniformed personnel, the administrative penalties may range from a letter of censure or reprimand to an Article 15. In the case of our civilian employees, they might range from an oral warning to a three-day suspension without pay or perhaps dismissal. The point is that the new Executive Order does abjure overclassification and adds some teeth to its warning.

Q. Mr. Liebling, has the declassification system changed significantly under the new directive?

A. Yes, very much so. We have shortened the time period for automatic

declassification from a normal 12-year schedule for Top Secret, Secret and Confidential to one where Top Secret would be downgraded in two years to Secret and from Secret it would be downgraded in an additional two years to Confidential and then declassified after an additional six years, whereas Secret will be downgraded to Confidential in two years and then declassified in an additional six. Confidential, in all cases, would be declassified after six years. So what you are talking about is from a 12-year base line under the old Executive Order, you now have a 6-, 8- and 10-year base line applied on a graduated basis, beginning with Confidential.

Q. How about the people who are involved in the declassification process, are they the same as are involved in the classification process?

A. (Mr. Liebling) No, not necessarily. There is a provision in the new Executive Order which provides for the heads of Agencies to name particular individuals other than those with classification authority to effect declassification. But, of course, like any system, a judicious application of the classification criteria is important. The emphasis that the program has recently received by the President, the Secretary and Deputy Secretary of Defense, by the Congress and the press, has provided for a discipline on the part of individuals and a consciousness toward meeting these declassification schedules. As Mr. Cooke has indicated, if it is impossible to establish a date or event in advance of the declassification schedule, then you use the schedule, so the attempt is being made to progressively downgrade and declassify on a more rapid basis.

Q. Recently, Mr. Liebling, we have had the release of the Pentagon Papers. Do you think this new Executive Order will prevent recurrences of this nature in the future?

A. It is an interesting question. Of course, I won't address myself to the Pentagon Papers because of the litigation aspects of the case. But on a general basis, my answer would be that you are dealing with a human error factor, and with the number of people who have access to classified information on a Government-wide basis or who have access while in service. It is a difficult action to police. You must rely on the integrity and trustworthiness of the individual who has been provided the access.

Q. There is the impression that an individual who leaves the Defense Department and who has in the past had access to classified material is free to go about divulging such information. What is to prevent this from happening?

A. (Mr. Cooke) Well, in the last analysis, the security of the system depends upon the integrity of each individual in the system. A civilian employee or a military member leaving the Defense establishment who has had a security clearance is debriefed. He customarily signs a statement promising not to divulge classified information, and in that regard, I think our track record is pretty good, perhaps as high as Ivory soap with 99.4 percent pure. Predictably, though, there are some who do divulge. The emphasis and attention of course is on the bad news, not the good news. Because the system is run by people for people, there will always be those who will abuse the system. All I can say is that we try our best to stop them and do take actions, as may be appropriate, in each individual case.

Q. Is the signing of the debriefing statement all there is to it? Are there any restrictions, post-employment wise, for service people or civil servants?

A. (Mr. Cooke) Within the Continental United States (CONUS) there are no restrictions in post-employment at all. In fact, I'm not so sure of the legality of such restrictions. There is, of course, a careful physical inventory to locate and properly dispose of all classified documents in your possession before you exit. But in answer to your question, there are no post-separation restrictions on type of employment.

Q. Could I travel to a Communist nation?

A. (Mr. Cooke) With certain very limited exceptions and depending upon the duty you had in the Service, you would be like any other American citizen and could go wherever you want. Here again the integrity of the system rests upon the judgment of the individual and we would hope that anyone who has had access to extremely sensitive information would exercise sound judgment in travelling overseas.

Mr. Liebling: I think it is also a question of jurisdiction. As far as the Department of Defense is concerned, our jurisdiction ends in most cases when a person leaves the Service. If you remember recent hearings regarding information gathering in the civilian community, this would probably be one of the aspects we would be concerned with in that we don't generally have that kind of a jurisdiction.

Q. Mr. Liebling, how closely is an individual screened before he is permitted to receive Top Secret or Secret information?

A. Procedures are established under other Executive Orders and DoD Directives for determining the reliability and trustworthiness of an individual. For example, for Secret we have what we call a National Agency Check, and for Top Secret we require a full background investigation. In the latter investigation we seek information regarding the individual's former employment, the schools he attended, and any possible FBI record. These and other similar checks are necessary, of course, in order to determine reliability.

Q. Can you give us any examples of what would exclude a person from being able to see classified documents?

A. (Mr. Liebling) Well, there are many factors. There is no categorical denial of a person for eligibility. In the event adverse information should emerge, such as criminal acts, alcoholism, or a mental type of problem without rehabilitation, these factors would most likely lead to our opening additional inquiry. However, in all cases a proper adjudication would be made as to the currency of the problem area. This program, of course, is designed with complete fairness to the individual in balancing the equities in behalf of national security interests and the rights of the individual. So, as I stated before, there isn't any categorical denial, as such.

Mr. Cooke: It might be somewhat analagous if you, as president of a bank, were deciding whether you should hire a new man as a teller in the bank. The standards may be a little higher in our own program because the interests of national security are involved, but this is the type of judgment that has to be brought to bear. I would like also to emphasize that the mere fact that you have a security clearance doesn't entitle you to receive classified information. A clearance merely means you are eligible to receive a particular level of classified. It is equally important that you must have a definite need-to-know for the particular information that you are receiving. For example, the mere fact that Mr. Liebling here has a Top Secret clearance doesn't mean he can automatically see any and all Top Secret papers in the

Office of the Secretary of Defense. He will be permitted to see only those Top Secret papers which, in the judgment of the people who have the papers in their possession, he has a need-to-know in the performance of his duties.

Mr. Liebling: In other words, regardless of the level of clearance we may hold, we are given access to only information we require in the performance of our duties. In fact, I myself, as head of a major DoD program, am not a Top Secret classification authority. Such policies, I feel, exemplify the integrity of the program as we are managing it now.

Q. Hasn't the prime factor in determining access to classified information always been the need-to-know?

A. (Mr. Cooke) You are correct, the need-to-know is not new. This principle has always been emphasized in our Defense security program. However, its importance has been brought into sharper focus as a result of the visibility that the new program has received.

Q. Does the new Directive deal with the granting of clearances to people or does it deal strictly with classification and declassification?

A. (Mr. Liebling) It has a section which deals with the clearance aspect but it does not go into extensive detail.

Mr. Cooke: Neither the new Directive nor the Executive Order is too specific on the subject of clearances. The authority to grant clearances, the criteria used, and the procedures used are spelled out in other Executive Orders and DoD Directives. The new Directive simply stresses the fact that before a clearance is granted, the recipient must be trustworthy. For more information on the actual clearance process, you will have to turn elsewhere.

Q. What about the man who is granted a Top Secret clearance in one job and later goes to a job where a Top Secret clearance is not required. Does he keep his Top Secret clearance?

A. (Mr. Cooke) No, he does not. The Top Secret clearance is related, of course, to the man's specific duties. If you had a Top Secret clearance and were ordered to a new duty station where you had no need for a Top Secret clearance, your clearance would be either downgraded (if a lower level of clearance were required) or if no access were involved, the clearance would be withdrawn. These are administrative actions, of course, and carry no derogatory connotation. This policy is merely a further extension of the need-to-know doctrine. Because if you are in a position where obviously you are not going to have a need-to-know anything classified, there is no reason for you to have a clearance. However, if you later moved to another duty station where a clearance was needed, it could be reinstated at the request of the command.

Mr. Liebling: It should be emphasized that the provisions for reinstatement of a clearance are applicable only so long as you remain within the Government. If you leave the Government, your clearance is terminated. We do have procedures, however, for transferring a clearance. For example, when a man leaves the DoD and is employed by a Defense contractor in private industry where he would require access to classified information, his clearance is transferable, that is, provided he assumes the new position within a particular time period.

Q. Mr. Liebling, how great is the incidence within DoD of documents being left unattended and thereby falling into hands of those who are unauthorized to have them?

A. First, you must remember that we are talking about several million people, both civilian and military, plus a large number in the Defense contracting community. Obviously because of such numbers, you will have administrative violations, as we call them, with a safe being left open or, as you suggest, cases where documents are exposed to unauthorized personnel. We recognize this problem, of course, and have established accountability procedures and other controls to minimize the occurrence of such incidents. For example, classified information which is extremely sensitive would only be in areas where the people going into that area would be cleared for access to the particular level of classified involved.

Q. So there would be no harm if, while in the areas, such persons should see a classified document?

A. (Mr. Liebling) Well, it is harm in the sense that he might be technically unauthorized to have access and the element of risk of compromise obviously would become greater. But, as Mr. Cooke has indicated before, we are talking in terms of possibly tens of millions of documents with relatively few incidents of exposure over the many years since the Department of Defense has been established.

Mr. Cooke: I would like to underscore that most of the so-called compromises or violations are not disclosures or deliberate leaks. They include in most cases such things as a safe being left open, the careless sticking of a classified document in a desk drawer, and other similar violations which are caused by sheer carelessness. Most of these things don't result in disclosure to persons other than our own security forces in the buildings where they are found. But it is these little things which hopefully we can cut down.

Q. As a final question, I'd like to ask each of you to address yourselves to this question—What do you consider to be most significant aspects of the new Executive Order and the DoD Regulation?

A. (Mr. Cooke) I think from the viewpoint of the public there will be more information released on an earlier basis, there will be less information classified, and there will be a greater impetus toward the release of information. From the viewpoint of someone in the organization, military or civilian, I think you can expect increased command attention at all levels to insure that not only the procedures but the spirit of the Executive Order and the Regulation are carried out.

Q. Can you add to that, Mr. Liebling?

A. Yes, I would agree with Mr. Cooke and would add that the program has received an emphasis, which, in my career in Government, it has never received before. We should not forget that the Secretary of Defense and the President personally met with people to direct this action. And I think the consciousness on the part of individuals, as I indicated earlier, is much more pronounced today, particularly in the management aspect of the program. We have mechanics for actually inspecting the compliance as well as the enforcement aspects of these programs, and we are developing education and indoctrination procedures to insure that this consciousness and respect for the program is maintained. All of these things we must do if we are to accomplish the President's objective which is to make the maximum amount of information available to the public and to protect only that information which is truly sensitive and is defined as classified information.

Selected Portions

New Security Regulation Details Explained (Part I)

The new Department of Defense Regulation governing the classification, downgrading, declassification and safeguarding of classified information was issued under the authority of and pursuant to DoD Directive 5200.1, Department of Defense Information Security Program, dated June 1, 1972. It is effective immediately and is applicable to all Department of Defense activities without the necessity of further formal issuance by any DoD component. The Service Secretaries may issue necessary supplementary instructions or directives to provide for the internal administration of the Regulation within their respective Services.

The Regulation has been approved by the Interagency Classification Review Committee as required by Executive Order 11652 and the National Security Council Directive issued pursuant thereto.

R. C. Moot

ROBERT C. MOOT
Assistant Secretary of Defense (Comptroller)

The following are selected excerpts from Chapters 1 through 4 and 13 of the new Regulation covering the classification management aspect, namely, classification, downgrading, declassification and marking, and field program management. The reader is cautioned that these excerpts do not cover the equally important safeguarding portions of the Regulation. These are found in Chapters 5 through 12, and deal with such matters as safekeeping, storage, dissemination, transmission and disposal requirements.

For a full authoritative explanation of the safeguarding as well as the classification management aspects of the new Information Security Program, consult DoD Information Security Program Regulation (ISPR) 5200.1-R.

CHAPTER I
GENERAL PROVISIONS
PURPOSE AND APPLICABILITY

Purpose

To ensure that official information of the Department of Defense relating to national security is protected, but only to the extent and for such period as is necessary, this Regulation establishes the bases for identification of information to be protected; prescribes a progressive system for classification, downgrading and declassification; prescribes safeguarding policies and procedures to be followed; and establishes a monitoring system to ensure the effectiveness of the Information Security Program throughout the Department of Defense.

Applicability

This Regulation governs the Department of Defense Information Security Program and takes precedence over all other departmental publications affecting that program.

Non-Government Operations

Except as otherwise provided herein, the provisions of this Regulation shall be made applicable by contract, or other legally binding instrument, to operations of non-government personnel entrusted or to be entrusted with classified information.

Combat Operations

The provisions of this Regulation with regard to accountability, dissemination,

DOD DIRECTIVE 5200.1

DOD INFORMATION SECURITY PROGRAM

JUNE 1, 1972

DOD INFORMATION SECURITY PROGRAM REGULATION
(DOD ISPR - DOD 5200.1-R)

July 15, 1972

EXECUTIVE ORDER 11652

BASIC GOVERNMENTAL POLICY

- THE INTERESTS OF THE UNITED STATES AND ITS CITIZENS ARE BEST SERVED BY MAKING INFORMATION REGARDING THE AFFAIRS OF GOVERNMENT READILY AVAILABLE TO THE PUBLIC.

- WITHIN THE FEDERAL GOVERNMENT THERE IS SOME OFFICIAL INFORMATION AND MATERIAL WHICH, BECAUSE IT BEARS DIRECTLY ON THE EFFECTIVENESS OF OUR NATIONAL DEFENSE AND THE CONDUCT OF OUR FOREIGN RELATIONS, MUST BE SUBJECT TO SOME CONSTRAINTS FOR THE SECURITY OF OUR NATION AND THE SAFETY OF OUR PEOPLE AND OUR ALLIES.

- TO PROTECT AGAINST ACTIONS HOSTILE TO THE UNITED STATES, OF BOTH AN OVERT AND COVERT NATURE, IT IS ESSENTIAL THAT SUCH INFORMATION AND MATERIAL BE GIVEN ONLY LIMITED DISTRIBUTION.

Richard M. Nixon
Washington, D.C., March 8, 1972

transmission, or safekeeping of classified information or material may be modified as necessary to meet local conditions by military commanders in connection with combat or combat-related operations. Classified information or material should be introduced into forward combat areas or zones only to the extent essential to accomplishment of the military mission. When so introduced, the appropriate military commander shall provide the degree of protection prescribed by this Regulation for the classification involved as nearly as the circumstances permit.

DEFINITIONS

As used herein, the following terms and meanings shall be applicable:

Classification

The determination that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made.

Classifier

An individual who either:

A. Determines that official information, not known by him to be already classified, currently requires, in the interests of national security, a specific degree of protection against unauthorized disclosure and, having the authority to do so, designates that official information as Top Secret, Secret or Confidential; or

B. Determines that official information is in substance the same as information known by him to be already classified by the Government as Top Secret, Secret or Confidential and designates it accordingly.

Declassification

The determination that classified information no longer requires, in the interests of national security, any degree of protection against unauthorized disclosure, coupled with a removal or cancellation of the classification designation.

Downgrade

To determine that classified information requires, in the interests of national

security, a lower degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such lower degree.

Official Information

Information which is owned by, produced for or by, or is subject to the control of the United States Government.

Original Classification Authority

Original classification authority is the authority to make original classifications vested specifically and in writing in an official of the Government as the incumbent of an office and in the official specifically and in writing designated to act in the absence of the incumbent.

CLASSIFICATION STANDARD

OFFICIAL INFORMATION AND MATERIAL SHALL BE CLASSIFIED WHEN UNAUTHORIZED DISCLOSURE THEREOF COULD REASONABLY BE EXPECTED TO CAUSE SOME DEGREE OF HARM TO THE INTERESTS OF THE NATIONAL DEFENSE OR FOREIGN RELATIONS OF THE UNITED STATES, WHICH ARE COLLECTIVELY TERMED "NATIONAL SECURITY".

Section 1, EO 11652

SECTION 4
POLICIES
Classification

A. **Basic Policy:** The Introduction to Executive Order 11652 states in part: "The interests of the United States and its citizens are best served by making information regarding the affairs of Government readily available to the public. This concept of an informed citizenry is reflected in the Freedom of Information Act and in the current public information policies of the executive branch.

"Within the Federal Government there is some official information and material which, because it bears directly on the effectiveness of our national defense and the conduct of our foreign relations, must be subject to some constraints for the security of our Nation and the safety of our people and our allies. To protect against actions hostile to the United States, of both overt and covert nature, it is essential that such official information and material be given only limited dissemination."

Consistent with the foregoing, the use and application of security classification shall be limited to only that information which is truly essential to national security because it provides the United States with: (a) a military or defense advantage over any foreign nation or group of nations, or (b) a favorable foreign relations posture or (c) a defense posture capable of successfully resisting hostile or destructive action from within or without, overt or covert; which could be damaged, minimized or lost by the unauthorized disclosure or use of the information.

B. **Resolution of Doubts.** Unnecessary classification and higher than necessary classification shall be scrupulously avoided. Any substantial doubts as to which of two levels of security classification is appropriate, or as to whether certain information or material should be classified at all, should be resolved in favor of the less restrictive treatment.

C. **Improper Classification:** Classification shall apply only to official information requiring protection in the interests of national security. It may not be used for the purpose of concealing administrative error or inefficiency, to prevent personal or departmental embarrassment, to restrain competition or independent initiative, or to prevent for any other reason the release of official information which does not require protection in the interests of national security.

Regrading and Declassification

In order to preserve the effectiveness and integrity of the Information Security Program, assigned classifications shall be responsive at all times to the current needs of national security. Classification, when determined to be required, shall be retained for the minimum length of time considering the degree of sensitivity, cost and probability of compromise. When classified information is determined, in the interests of national security, to require a different level of protection than that presently assigned, or no longer to require any such protection, it shall be regraded or declassified.

Safeguarding

Official information or material classified under the provisions of this Regulation shall be afforded the level of protection against unauthorized disclosure commensurate with the level of classification assigned under the varying conditions which may arise in connection with its use, dissemination, storage, movement or transmission and destruction.

SECTION 5
SECURITY CLASSIFICATION CATEGORIES

General

Official information or material which requires protection against unauthorized disclosure in the interests of national security shall be classified in one of three categories, namely, "Top Secret," "Secret," or "Confidential," depending upon the degree of its significance to national security. No other categories shall be used to identify official information or material as requiring protection in the interests of national security, except as otherwise expressly provided by statute.

Top Secret

Top Secret refers to that national security information or material which requires the highest degree of protection. The test for assigning Top Secret classification shall be whether its unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Examples of "ex-

ceptionally grave damage" include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security. This classification shall be used with the utmost restraint.

Secret

Secret refers to that national security information or material which requires a substantial degree of protection. The test for assigning Secret classification shall be whether its unauthorized disclosure could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security. The classification "Secret" shall be sparingly used.

Confidential

Confidential refers to that national security information or material which requires protection. The test for assigning Confidential classification shall be whether its unauthorized disclosure could reasonably be expected to cause damage to the national security.

SECTON 6
AUTHORITY TO CLASSIFY, DOWNGRADE AND DECLASSIFY

Original Classification Authority

The authority for making original classification determinations shall be restricted solely to those officials specifically designated in writing pursuant to the provisions of this Regulation, including the officials who are specifically designated in writing to act in their absence. These designations shall be limited to the minimum number absolutely required for efficient administration. Such officials may classify information or material only at the level authorized or below. This authority is personal to the incumbent of the designated office and may not be delegated.

CLASSIFICATION CATEGORIES

TOP SECRET -- EXCEPTIONALLY GRAVE DAMAGE TO THE NATIONAL SECURITY

TO BE USED WITH UTMOST RESTRAINT

Examples: Armed hostilities against US or allies

Disruption of vital foreign relations

Compromise -- Vital national defense plans
Complex cryptologic systems
Vital intelligence systems
Sensitive intelligence operations

Vital scientific and technological developments

SECRET -- SERIOUS DAMAGE TO THE NATIONAL SECURITY

TO BE USED SPARINGLY

Examples: Disruption of significant foreign relations

Significant impairment of programs or policy

Compromise significant scientific and technological developments

CONFIDENTIAL -- DAMAGE TO THE NATIONAL SECURITY

NOTE: No one is an original classification authority unless (1) he is the current incumbent of an official DoD position which has been specifically designated in writing as one, the incumbent of which has original classification authority at a particular level or levels, Top Secret, Secret or Confidential, or (2) he is the official specifically designated in writing to act in the absence of the aforesaid incumbent.

Record and Report Requirements

Records and reports of designations of original classification authority shall be maintained and submitted as follows:

A. Top Secret Listings. The Office of the Assistant Secretary of Defense (Comptroller), for (a) the Office of the Secretary of Defense, (b) the Organization of the Joint Chiefs of Staff, (c) the unified and specified commands, and (d) the Defense Agencies, shall maintain currently a listing of the officials by title, designated to exercise Top Secret original classification authority in those organizations. The offices named shall advise the Assistant Secretary of Defense (Comptroller) of any changes deemed necessary in the designations made. The Offices of the Secretaries of the Military Departments shall maintain lists of the officials by title in their respective departments designated to exercise original Top Secret classification authority.

B. Secret and Confidential Listings. The head of each Department of Defense component, the Office of the Assistant Secretary of Defense (Comptroller) acting for the Office of the Secretary of Defense, the Director, Joint Staff acting for the Organization of the Joint Chiefs of Staff, and the Commanders in Chief of unified and specified commands for their respective headquarters, shall maintain listings by title of the officials designated to exercise Secret and Confidential original classification authority in their respective organizations.

Currency of Designations

Designations of original classification

authorities shall be kept current by written action of the officials authorized to make such designations.

Reports

The Military Departments shall submit by July 1, 1972, to the Deputy Assistant Secretary of Defense (Security Policy) a listing by title of the officials designated to exercise Top Secret original classification authority. The heads of all Department of Defense components, as indicated in subparagraph B, of Record and Report Requirements above, shall submit to the Deputy Assistant Secretary of Defense (Security Policy) by July 1, 1972, the listings by title of the officials in their respective organizations who have been designated to exercise Secret and Confidential original classification authority. Changes in such reports shall be submitted quarterly beginning October 1, 1972.

Downgrading and Declassification Authority

Original classification authorities or higher officials in the same chain of command or supervisory responsibility are authorized to downgrade or declassify information classified by the original classifier. In addition, to the maximum extent practicable, heads of Department of Defense components shall establish procedures by which officials are designated at headquarters level who are authorized to downgrade and declassify information under the classification jurisdiction of any subordinate offices or echelons and to resolve conflicts or doubts as to the classifications that are appropriate as of current date.

". . . It is vitally important that DoD personnel everywhere, *military and civilian, be well* versed in the new system and put it to practice to the best of their ability. . . ."

—Melvin R. Laird
Secretary of Defense

CLASSIFICATION AUTHORITIES

TOP SECRET

AUTHORIZED BY EXECUTIVE ORDER 11652

SECRETARY OF DEFENSE

SECRETARY OF THE ARMY

SECRETARY OF THE NAVY

SECRETARY OF THE AIR FORCE

1. Senior principal deputies and assistants to Secretaries
2. Heads of major elements of DoD

Senior principal deputies and assistants to heads

SECRET

DESIGNATED TOP SECRET AUTHORITIES

OFFICIALS DESIGNATED BY THE FOUR SECRETARIES

OFFICIALS DESIGNATED BY FIRST GROUP OF TOP SECRET DESIGNEES

CONFIDENTIAL

DESIGNATED TOP SECRET AND SECRET AUTHORITIES

OFFICIALS DESIGNATED BY TS AND S AUTHORITIES

INITIALLY, S AND C DESIGNATIONS BY FOUR SECRETARIES

DOWNGRADING AND DECLASSIFICATION

AUTHORITY -- ORIGINAL CLASSIFIERS
HIGHER AUTHORITIES
DESIGNATED OFFICIALS

RESPONSIBILITY -- ALL PERSONS

CHAPTER II
CLASSIFICATION
SECTION I
CLASSIFICATION RESPONSIBILITIES

Accountability of Classifiers

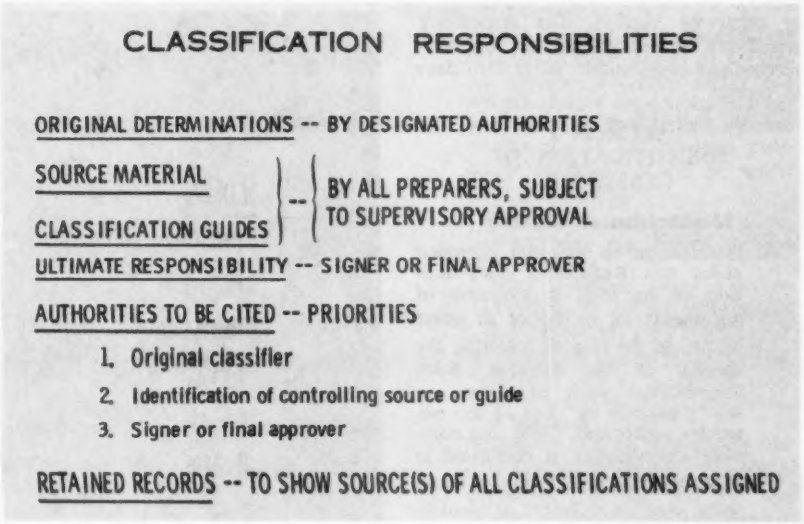
Each classifier shall be held accountable for the propriety of the classifications assigned by him, whether in the exercise of original classification authority or in the determination and application of classifications assigned in source documents or as prescribed by applicable classification guidance, and shall maintain adequate records to support his actions. Such records could take the form of an approved security classification guide or a notation on the record copy of the classified document indicating the source of the classification or, if an original classification, a brief justification for the classification determination. In any case, the classifier is required to maintain a record to show the basis for classification or by which the chain of classification authority can be traced to an original classification authority who can justify the initial classification determination, should an occasion demand such action. An official with the requisite classification authority who classifies a document or other material and who identifies himself thereon as the classifier, is, and continues to be, the accountable classifier, even though the document or material is finally approved or signed at a higher level in the same organization.

Classification Review

A. When an official signs or finally approves a document or other material already marked to reflect a particular level of classification, he shall review the information contained therein to determine if the classification marking(s) is (are) appropriate. If, in his judgment, the classification marking(s) is (are) not supportable, he shall cause such marking(s) to be removed or changed as appropriate to reflect accurately the classification of the information involved prior to issuance.

B. A higher level official through or to whom a document or other material passes for signature or final approval becomes jointly responsible with the accountable classifier for the classification(s) assigned. In any particular organization a determination as to whether the higher level official wishes to have his subordinates who have requisite classification authority to be shown as the accountable classifier is a matter for internal management to decide.

C. If no one is specifically identified as the classifier, the official who finally signs or approves the document or other material is the accountable classifier.


CLASSIFICATION RESPONSIBILITIES
ORIGINAL DETERMINATIONS -- BY DESIGNATED AUTHORITIES
SOURCE MATERIAL
CLASSIFICATION GUIDES
--
BY ALL PREPARERS, SUBJECT TO SUPERVISORY APPROVAL
ULTIMATE RESPONSIBILITY -- SIGNER OR FINAL APPROVER
AUTHORITIES TO BE CITED -- PRIORITIES
1. Original classifier
2. Identification of controlling source or guide
3. Signer or final approver
RETAINED RECORDS -- TO SHOW SOURCE(S) OF ALL CLASSIFICATIONS ASSIGNED

Classification Planning

Advance classification planning is an essential part of the development of any plan, operation, program, research and development project, or procurement action in which security is a major factor, or which involves classified information. The classification aspects must be considered from the beginning to assure adequate protection for the information and for the activity itself, and to eliminate impediments to the execution or implementation of the plan, operations order, program, project, or procurement action.

The commander or official charged with the development of any plan, program or project, in which classification is a factor, shall include therein, under a clearly identifiable title or heading, a classification guide covering the information involved in that effort or a classification plan, prepared by qualified personnel who have at hand the necessary knowledge and technical intelligence to make reasonable determinations covering the following:

A. Isolation and identification of information involved in the effort which requires classification.

B. Classification guidance specifying the levels of classification to be applied to identified items of information and material developed in connection with the plan, program or project.

C. A schedule for phased downgrading and declassification covering each item of classified information and material.

D. Provision for periodic review to determine the currency and accuracy of the classification, downgrading, and declassification guidance provided.

Recipient of Classified Information or Material

If the recipient of classified information or material has reason to believe that it should not be classified or that current security considerations justify a change in the assigned classification, he shall make such changes if he is authorized to do so. If not so authorized, he shall promptly submit the matter to the appropriate classifier with his recommendations and reasons therefor. Pending final determination, the material shall be safeguarded as required for its assigned or proposed classification, whichever is higher, until the classification is changed

authorities shall be kept current by written action of the officials authorized to make such designations.

Reports

The Military Departments shall submit by July 1, 1972, to the Deputy Assistant Secretary of Defense (Security Policy) a listing by title of the officials designated to exercise Top Secret original classification authority. The heads of all Department of Defense components, as indicated in subparagraph B. of Record and Report Requirements above, shall submit to the Deputy Assistant Secretary of Defense (Security Policy) by July 1, 1972, the listings by title of the officials in their respective organizations who have been designated to exercise Secret and Confidential original classification authority. Changes in such reports shall be submitted quarterly beginning October 1, 1972.

Downgrading and Declassification Authority

Original classification authorities or higher officials in the same chain of command or supervisory responsibility are authorized to downgrade or declassify information classified by the original classifier. In addition, to the maximum extent practicable, heads of Department of Defense components shall establish procedures by which officials are designated at headquarters level who are authorized to downgrade and declassify information under the classification jurisdiction of any subordinate offices or echelons and to resolve conflicts or doubts as to the classifications that are appropriate as of current date.

> ". . . It is vitally important that DoD personnel everywhere, military and civilian, be well versed in the new system and put it to practice to the best of their ability. . . ."
>
> —Melvin R. Laird
> Secretary of Defense

CLASSIFICATION AUTHORITIES

TOP SECRET

AUTHORIZED BY EXECUTIVE ORDER 11652

SECRETARY OF DEFENSE

SECRETARY OF THE ARMY

SECRETARY OF THE NAVY

SECRETARY OF THE AIR FORCE

1. Senior principal deputies and assistants to Secretaries
2. Heads of major elements of DoD

Senior principal deputies and assistants to heads

SECRET

DESIGNATED TOP SECRET AUTHORITIES

OFFICIALS DESIGNATED BY THE FOUR SECRETARIES

OFFICIALS DESIGNATED BY FIRST GROUP OF TOP SECRET DESIGNEES

CONFIDENTIAL

DESIGNATED TOP SECRET AND SECRET AUTHORITIES

OFFICIALS DESIGNATED BY TS AND S AUTHORITIES

INITIALLY, S AND C DESIGNATIONS BY FOUR SECRETARIES

DOWNGRADING AND DECLASSIFICATION

AUTHORITY -- ORIGINAL CLASSIFIERS
HIGHER AUTHORITIES
DESIGNATED OFFICIALS

RESPONSIBILITY -- ALL PERSONS

CHAPTER II
CLASSIFICATION
SECTION I
CLASSIFICATION RESPONSIBILITIES

Accountability of Classifiers

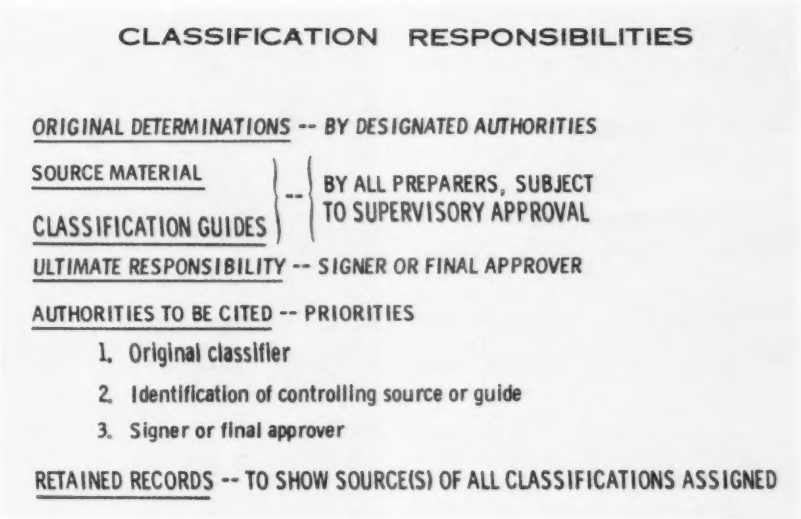
Each classifier shall be held accountable for the propriety of the classifications assigned by him, whether in the exercise of original classification authority or in the determination and application of classifications assigned in source documents or as prescribed by applicable classification guidance, and shall maintain adequate records to support his actions. Such records could take the form of an approved security classification guide or a notation on the record copy of the classified document indicating the source of the classification or, if an original classification, a brief justification for the classification determination. In any case, the classifier is required to maintain a record to show the basis for classification or by which the chain of classification authority can be traced to an original classification authority who can justify the initial classification determination, should an occasion demand such action. An official with the requisite classification authority who classifies a document or other material and who identifies himself thereon as the classifier, is, and continues to be, the accountable classifier, even though the document or material is finally approved or signed at a higher level in the same organization.

Classification Review

A. When an official signs or finally approves a document or other material already marked to reflect a particular level of classification, he shall review the information contained therein to determine if the classification marking(s) is (are) appropriate. If, in his judgment, the classification marking(s) is (are) not supportable, he shall cause such marking(s) to be removed or changed as appropriate to reflect accurately the classification of the information involved prior to issuance.

B. A higher level official through or to whom a document or other material passes for signature or final approval becomes jointly responsible with the accountable classifier for the classification(s) assigned. In any particular organization a determination as to whether the higher level official wishes to have his subordinates who have requisite classification authority to be shown as the accountable classifier is a matter for internal management to decide.

C. If no one is specifically identified as the classifier, the official who finally signs or approves the document or other material is the accountable classifier.


CLASSIFICATION RESPONSIBILITIES
ORIGINAL DETERMINATIONS -- BY DESIGNATED AUTHORITIES
SOURCE MATERIAL
CLASSIFICATION GUIDES
-- BY ALL PREPARERS, SUBJECT TO SUPERVISORY APPROVAL
ULTIMATE RESPONSIBILITY -- SIGNER OR FINAL APPROVER
AUTHORITIES TO BE CITED -- PRIORITIES
1. Original classifier
2. Identification of controlling source or guide
3. Signer or final approver
RETAINED RECORDS -- TO SHOW SOURCE(S) OF ALL CLASSIFICATIONS ASSIGNED

Classification Planning

Advance classification planning is an essential part of the development of any plan, operation, program, research and development project, or procurement action in which security is a major factor, or which involves classified information. The classification aspects must be considered from the beginning to assure adequate protection for the information and for the activity itself, and to eliminate impediments to the execution or implementation of the plan, operations order, program, project, or procurement action.

The commander or official charged with the development of any plan, program or project, in which classification is a factor, shall include therein, under a clearly identifiable title or heading, a classification guide covering the information involved in that effort or a classification plan, prepared by qualified personnel who have at hand the necessary knowledge and technical intelligence to make reasonable determinations covering the following:

A. Isolation and identification of information involved in the effort which requires classification.

B. Classification guidance specifying the levels of classification to be applied to identified items of information and material developed in connection with the plan, program or project.

C. A schedule for phased downgrading and declassification covering each item of classified information and material.

D. Provision for periodic review to determine the currency and accuracy of the classification, downgrading, and declassification guidance provided.

Recipient of Classified Information or Material

If the recipient of classified information or material has reason to believe that it should not be classified or that current security considerations justify a change in the assigned classification, he shall make such changes if he is authorized to do so. If not so authorized, he shall promptly submit the matter to the appropriate classifier with his recommendations and reasons therefor. Pending final determination, the material shall be safeguarded as required for its assigned or proposed classification, whichever is higher, until the classification is changed

or otherwise verified. The responsible classifying authority shall act on such recommendations within thirty (30) days of receipt.

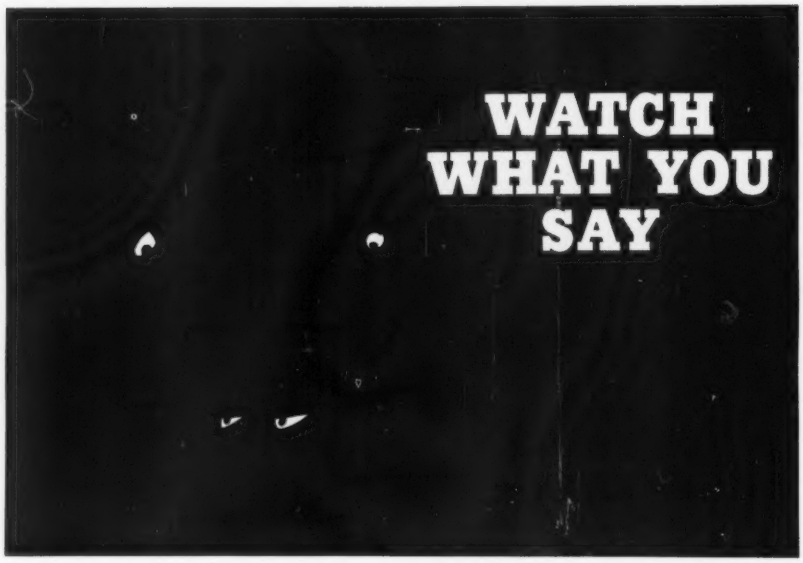
SECTION 2
IDENTIFICATION OF CLASSIFIER

Identification of Classifier

A. Information or material classified under this Regulation shall indicate on its face, in the case of documents, or by notice or other means, in the case of material, the identity of the classifier. Such identification shall be shown on the "Classified by" line of the notations authorized. Clear and complete identification is construed to mean that the description standing alone shall be sufficient to identify a particular official, source document or classification guide, as the case may be. Identification of a source document or guide will include the date thereof and the title and organization of the original classifier, when known.

1. If all of the information in the document or other material is classified as an act of original classification, the official with requisite classification authority who made the classification determination shall be identified on the face of the document in the "Classified by" space by his title and position in his organization.
2. If all of the classified information contained in a document is classified because of classification imposed by a single outside source, for example, a source document or classification guide, and no original classification is involved, the "Classified by" line will identify the source document or guide, including its date, and also the official title and organization of the original classifier, when known.
3. If the classified information contained in a document or other material is classified because of classifications imposed by more than one outside source document, classification guide or combination thereof, the official title and position of the signer or final approver of the new document or other material shall be shown in the "Classified by" space.
4. If a particular official has been designated by the head of an organization to be the approver of the security classification assigned to all classified material leaving the organization, the official title and position of that designated official shall be shown in the "Classified by" space.

B. In all of the situations in 1 through 4 above, the official responsible for completing the "Classified by" line in the stamp shall establish and retain adequate records to support his action.



SECTION 3
CLASSIFICATION PRINCIPLES, CRITERIA AND CONSIDERATIONS

Balanced Judgment Requirement

Classification is a balanced judgment. There must be a positive basis for classification, but both advantages and disadvantages to classifying must be considered. Determination to classify shall not be made and a classification marking shall not be applied until after full consideration of both aspects. All paragraphs of this section must be considered before a classification determination is made or a classification marking is applied.

Identification of Specific Information

Classification determinations must be preceded by an exact identification of each item of information which may require security protection in the interests of national security. This process involves identification of that specific information which comprises the basis for the particular national advantage or advantages which, if the information were compromised, would or could be damaged, minimized, or lost, thereby adversely affecting the national security.

Reasons for Classification

An evaluation of information forms the base for classification. A document or other material is classified either: (1) because of the information it contains, which may be ascertained by study, analysis, observation or use of it; or (2) because of the information it may reveal when associated with other information, including that which the classifier knows already has been officially released into the public domain.

Specific Classifying Criteria

A determination to classify shall be made only when one or more of the following considerations are present *and the unauthorized disclosure of the information could reasonably be expected to cause a degree of harm to the national security:*

A. The information provides the United States, in comparison with other nations, with a scientific, engineering, technical, operational,

intelligence, strategic or tactical advantage directly related to the national security.

B. Disclosure of the information would weaken the position of the United States in the discussion, avoidance or peaceful resolution of potential or existing international differences which could otherwise generate a military threat to the United States or its mutual security arrangements, create or increase international tensions contrary to the national security of the United States, result in a disruption in foreign relations, or lead to hostile political or military action against the United States or its allies, thereby adversely affecting the national security.

C. Disclosure of the information would weaken the ability of the United States to wage war or defend itself successfully, limit the effectiveness of the armed forces, or make the United States vulnerable to attack.

D. There is sound reason to believe that other nations do not know that the United States has, or is capable of obtaining, certain information or material which is important to the national security of the United States vis-a-vis those nations.

E. There is sound reason to believe that knowledge of the information would: (a) provide a foreign nation with an insight into the war potential or the war or defense plans or posture of the United States; (b) allow a foreign nation to develop, improve or refine a similar item of war potential; (c) provide a foreign nation with a base upon which to develop effective countermeasures; (d) weaken or nullify the effectiveness of a defense or military plan, operation, project or activity which is vital to the national security.

Dissemination Considerations

The degree of intended or anticipated dissemination and use of material, and whether the end purpose to be served renders effective security control impractical, are factors which must be considered. These factors do not necessarily preclude classification, but they do force consideration of the extent to which classification under such circumstances may degrade the classification system by attempting to impose security control in impractical situations.

Net National Advantage

In exceptional circumstances involving scientific and technical information or material, it may be necessary to weigh the benefits which would accrue to the United States generally from the unclassified use by other United States government agencies or commercial interests of information which is classified or otherwise classifiable under this Regulation, against the advantage by classification or continued classification of the information. When a net advantage to the United States resulting from unclassified use distinctly can be ascertained beyond a reasonable doubt, that factor should be considered in reaching the classification determination.

Lead Time Advantage

A. Lead time is the interval between the acquisition of knowledge by or on behalf of the Government of the United States and the time when the Government of the United States believes that the same knowledge is known to, or reasonably could be known to, the private community in the United States or to other nations through the application of their own resources.

B. The United States as a nation may have a sufficient edge on a sufficiently broad basis of technical competence over other nations that an essential national defense lead time advantage might be obtained or maintained through an open race with other nations.

C. If it is reasonably believed that an essential national defense lead time advantage can be obtained or maintained as well or better through reliance upon the total available U.S. technological base, open circulation, after public release approval, will be preferred to security classification.

D. If it is reasonably believed that an essential national defense lead time advantage which could be obtained or maintained through security classification more than likely would be lost through open circulation after public release approval, the determination will be to use security classification.

Cost Factor

Cost alone is not a positive basis for classification. Cost may be a reason for not classifying under certain conditions as shown below.

A. If cost resulting from classification in terms of time, money or personnel becomes a critical factor and actually might impede or prevent attainment of the desired mission or objective of the program, project or operation, it will be necessary to consider:
   1. Value to national defense of accomplishing the desired mission or objective.
   2. Risk attendant upon non-classification of certain information in order to attain the desired goal.
   3. Maximum extent to which classification can be employed without actually impeding attainment of the goal.

B. Whenever officials responsible for carrying out a program, project or operation consider that the cost factor resulting from classification may impede or prevent attainment of the desired mission or objective, the matter shall be referred, with appropriate explanations and recommendations, to the original classifying authority for the program, project or operation.

C. Final determinations of the effect of the cost factor on classification under circumstances set forth in paragraph B., above, shall be made only at or above the level of the original classifying authority for the program, project or operation.

Classifying Research Data

Ordinarily, except for information which meets the definition of Restricted Data, basic scientific research or results thereof shall not be classified.

Classifying Documents

Each document shall be classified on the basis of the information it contains or reveals. The fact that a document makes reference to a classified document is not a basis for classification unless the reference, standing alone, reveals classified information. The overall classification of a document, file, or group of physically connected documents shall be at least as high as that of the most highly classified component. Each component, however, shall be classified individually on its own merits.

Classifying Material Other Than Documents

Items of equipment or other physical

objects may be classified only when classified information may be derived from them by visual observation of internal or external appearance, structure, operation, test, application or use. The overall classification assigned to equipment or physical objects shall be at least as high as the highest classification of any of the items of information revealed by the equipment or objects.

State-of-the-Art and Inteliigence

Classification requires consideration of the information available from intelligence sources concerning the extent to which the same or similar information is known or is available to others. It is also important to consider whether it is known, publicly or internationally, that the United States has the information or even is interested in the subject matter. The state-of-the-art in other nations is a vital factor requiring consideration.

Effect of Open Publication

Appearance in the public domain of information currently classified or being considered for classification does not preclude initial or continued classification; however, such disclosures require immediate re-evaluation of the information to determine whether the publication has so compromised the information that downgrading or declassification is warranted. Similar consideration must be given to related items of information in all programs, projects or items incorporating or pertaining to the compromised items of information. In these cases, if the release is shown to have been made or authorized by an official Government source, classification of clearly identified items shall no longer be continued. However, holders should continue classification until advised to the contrary by a competent Government authority. Under no circumstances may a compilation of official public releases be classified.

Re-evaluation of Classification Because of Compromise

Specific classified information subjected to compromise or possible compromise and information related thereto shall be re-evaluated and acted upon as follows:

A. The original classifying authority, upon learning that a compromise or possible compromise of specific classified information has occurred, shall:

1. Re-evaluate the information involved and determine whether: (a) the classification should be continued without changing the specific information involved; (b) the specific information, or parts thereof, should be modified to minimize or nullify the effects of the reported compromise and the classification retained; (c) immediate downgrading is appropriate; (d) the original schedule specified for downgrading the information involved should be changed to reflect an earlier downgrading time; or (e) declassification is warranted.

2. When such determination is within categories (b), (c), (d) or (e) of above subparagraph, give prompt notice thereof to all holders of such information.

B. Upon learning that a compromise or possible compromise of specific classified information has occurred, any official having original classification jurisdiction over related information shall re-evaluate the related information and determine whether one of the courses of action enumerated in paragraph A. 1., above, should be taken or, in lieu thereof, upgrading of the related information is warranted. When such a determination is within categories (b), (c), (d) or (e) of paragraph A. 1., above, or that upgrading of the related items is warranted, prompt notice of the determination shall be given to all holders of the related information.

Compilation of Information

The general rule is that a compilation of unclassified items shall not be classified. In rare and unusual circumstances, however, classification may be required if the combination of unclassified items together provides an added factor which warrants classification. Classification on this basis shall be used sparingly.

Extracts of Information

Information or material extracted from a classified source will be classified, or not classified, as the case may be, in accordance with the classification markings shown in the source. The overall

CLASSIFICATION POLICIES

DO

CLASSIFY ONLY TO PROTECT NATIONAL SECURITY INTERESTS

CHOOSE THE LESS RESTRICTIVE ACTION

DECLASSIFY AS SOON AS POSSIBLE

DON'T

CLASSIFY FOR REASONS NOT AFFECTING NATIONAL SECURITY

OVERCLASSIFY

UNDERCLASSIFY

CLASSIFY TO CONCEAL ADMINISTRATIVE ERROR OR INEFFICIENCY

CLASSIFY TO PREVENT PERSONAL OR DEPARTMENTAL EMBARRASSMENT

CLASSIFY TO RESTRAIN COMPETITION OR INDEPENDENT INITIATIVE

marking and internal markings of the source should supply adequate classification guidance to the person making the extraction.

SECTION 4
CLASSIFICATION GUIDES

General

A classification guide, based upon classification determinations made by appropriate classification authorities, shall be issued for each system, program or project. Successive operating echelons shall prescribe any further detailed supplemental guides deemed essential to assure accurate, uniform and consistent classification.

Review of Classification Guides

Classification guides shall be reviewed by the originator for currency and accuracy not less often than once each year. Changes shall be issued promptly to all holders.

Sufficiency of Classification Guides

Classification guides must be sufficiently detailed to identify the critical items of information which require classification and yet sufficiently flexible to assure accurate classification of documentation and other material developed at various levels and during different stages of the program or project. It is particularly important that such guides not result in stagnation and overclassification through automatic application of their content.

SECTION 5
RESOLUTION OF CONFLICTS

General

When two or more offices, headquarters or activities disagree concerning a classification, declassification, or regrading action, the disagreement must be resolved promptly. Normally, mutual consideration by the offices, headquarters or activities concerned of the arguments for and against classification will provide adequate basis for reaching agreement.

Procedures

If agreement cannot be reached at the operating level, the matter shall be referred for decision to the lowest superior common to the disagreeing parties. If agreement cannot be reached at the major command (or equivalent) level, the matter shall be referred for decision to the headquarters office having overall classification management responsibilities for the component.

Timing

Action at each level of consideration on any disagreement on a classification, declassification or regrading problem shall be completed as soon as possible but within thirty (30) days. Failure to reach decision within thirty (30) days shall be cause for referral to the next higher echelon.

SECTION 6
OBTAINING CLASSIFICATION EVALUATIONS

Tentative Classification

If a person not authorized to classify originates or develops information which he believes should be safeguarded, he shall:

A. Safeguard the information in the manner prescribed for the intended classification.

B. Mark the information (or cover sheet) with a *tentative* classification (e.g., "Tentative Confidential").

C. Forward the material to an appropriate classifying authority for evaluation and decision. If such authority is not readily identifiable, the material should be forwarded to a headquarters activity of a Department of Defense component, to the headquarters office having overall classification management responsibilities for a Department of Defense component or to the Deputy Assistant Secretary of Defense (Security Policy) (DASD-[SP]).

D. In an emergency requiring immediate communication of the information, after taking the action prescribed by A and B, above, transmit the information and then proceed in accordance with C, above.

Upon decision by the classifying authority, the tentative marking shall be removed. If a classification has been assigned, appropriate markings shall be applied as prescribed by this Regulation.

SECTION 7
PRIVATE INFORMATION

General

Although only official information may be classified, there are some circumstances in which information not meeting the definition of official information may warrant protection in the interest of national security.

Independent Research and Development

A. The product of independent research and development shall not be classified unless the product incorporates classified information to which the person or the company was given prior access.

B. Independent research and development may be Government-sponsored, or may be a purely private, unsponsored effort. Government-sponsored independent research and development may be done by a person who, or company which, previously was given access to classified information. If no prior access was given, classification is not permissible unless the government first acquires a proprietary interest.

Other Private Information

In any other instance, for example, an unsolicited bid, in which a firm, organization, or individual submits to the government private information for determination of classification, the steps specified in Section 6, above, shall be taken.

SECTION 8
UPGRADING

Raising to a Higher Level of Classification

Upgrading classified information to a higher level than previously determined is permitted only when it is determined by the upgrading authority that:

A. All holders of the information are authorized access to the higher classification category;

B. All holders of the information can be promptly notified of the upgrading; and

C. Any dissemination to holders not authorized access to the higher classification category can be neutralized through retrieval.

Classification of Information Previously Determined to be Unclassified

Unclassified information, once communicated as such, is permitted to be classified only when the classifying authority makes the same determination described for upgrading in the preceding paragraph above and, in addition, determines that control of the information has not been lost by such communication

and can still be prevented from being lost.

Information Released to Secondary Distribution Centers

No attempt shall be made to classify information previously determined to be unclassified which is contained in documents released to secondary distribution centers, such as the Defense Documentation Center, unless it is determined that no secondary distribution has been made and can still be prevented.

Notification

Notification of upgrading or the classification of information previously determined to be unclassified shall not be given to holders from whom retrieval is accomplished.

SECTION 9
INDUSTRIAL OPERATIONS

Classification in Industrial Operations

Classification in industrial operations shall be based strictly on security classification guidance furnished by the Government. Industrial management does not make original classification determinations but applies the classification decisions of the contracting authority with respect to information and material developed, produced or handled by the contracting facility itself. Industrial management shall designate persons who shall have the responsibility for assuring that Government security classification guidance is applied accurately and uniformly. Numbers of persons authorized to determine the proper classifications to be applied in accordance with the government guidance shall be limited to the minimum consistent with operational requirements.

CHAPTER III
DOWNGRADING AND DECLASSIFICATION
SECTION 1
GENERAL PROVISIONS

Downgrading and Declassification Determinations

When a classification determination is made, it is necessary to determine how long the classification shall last in accordance with the policy expressed in Regarding and Declassification (Page 8). Classified information and material shall be downgraded and declassified as soon as there are no longer any grounds for continued classification within the classification category definitions set forth in the section on Security Classification Categories (Page 8), and the classification principles, criteria and considerations set forth in the section on Classification Principles, Criteria and Considerations (Chapter II, Section 3, Page 12).

Priority Consideration of Earliest Possible Date or Event

The individual exercising original classifying authority shall, to the maximum extent practicable, predetermine at the time of origination, dates or events on which downgrading and declassification shall occur. These dates or events shall be as early as the national security will permit. The dates of the General Declassification Schedule as set forth below shall not be used unless an Advanced Declassification Schedule for dates or events earlier than the General Declassification Schedule cannot be predetermined.

Dates or Events Carried Forward

Downgrading and declassification dates or events under the preceding paragraph above, or dates scheduled under the General Declassification Schedule below, shall be carried forward and applied whenever the classified information is incorporated in later documents or other material.

". . . Simply stated, it provides for the classification of less information plus the declassification of more information plus a monitoring system for effective compliance. The principal objective of the new regulation is, of course, to make the greatest amount of information available to the public. . . ."

—Joseph J. Liebling
Deputy Assistant Secretary of Defense
(Security Affairs)

". . . In the last analysis, the security of the system depends upon the integrity of each individual in the system. . . ."

—David O. Cooke
Deputy Assistant Secretary of Defense
(Administration)

The concluding portion of selected chapters from the new DoD Information Security Program Regulation, DoD 5200.1-R, July 15, 1972 will be published in COMMANDERS DIGEST, Vol. 13, No. 3, dated November 23, 1972.

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.
Price 5 cents (single copy). Subscription Price: $2.50 per year; $2.00 additional for foreign mailing.
☆ U.S. GOVERNMENT PRINTING OFFICE 513/344/X-25